

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X
UNITED STATES OF AMERICA,

– against –

No. 21-cr-110 (NGG)

JACOB DASKAL,

Defendant.

**DEFENDANT JACOB DASKAL’S MEMORANDUM OF LAW
IN SUPPORT OF HIS OMNIBUS PRETRIAL MOTIONS**

MEISTER SEELIG & FEIN, LLP

Attorneys for Jacob Daskal

125 Park Avenue, 7th Floor

New York, New York 10017

Phone: (212) 655-3500

Fax: (212) 655-3535

TABLE OF CONTENTS

I.	PRELIMINARY STATEMENT	1
II.	THE SEARCHES OF MR. DASKAL’S PHONES ARE INDELLIBLY TAINTED BY THE STATE AUTHORITIES’ PRIOR UNCONSTITUTIONAL SEARCH, REQUIRING SUPPRESSION OF all fruits OF thOSe searches	3
A.	The New York State Supreme Court Found the NY Phones Warrant Unconstitutionally Overbroad and Lacking Particularity	4
B.	The Government Should Be Collaterally Estopped from Contesting the State Court’s Suppression Order.....	5
C.	Alternatively, This Court Should Independently Find the NY Phones Warrant Constituted an Unconstitutional “General Warrant” in Violation of the Fourth Amendment, Requiring Suppression of All Evidence Seized From the Phones	8
1.	The NY Phones Warrant Was Overbroad.....	8
2.	The NY Phones Warrant Lacked Particularity	9
D.	The Unreasonable Five-Month Delay Between Seizure and Warrant Also Requires Suppression Under <i>Smith</i>	11
E.	The Subsequent Federal Phones Warrant Relied Upon Tainted Evidence, and Therefore Cannot Be Relied Upon to Provide the Lawful Basis to Avoid Suppression of Seized Evidence From the Daskal Phones.....	13
III.	THE COURT SHOULD SUPPRESS THE FRUITS OF THE SEARCHES ON MR. DASKAL’S PHONES AND COMPUTERS: THE FEDERAL WARRANTS WERE OVERBROAD AND THE AGENTS HELD THE DEVICES AND FAILED TO CONDUCT TIMELY RESPONSIVENESS REVIEWS	15
A.	The Government Conducted Continuous Searches of the Daskal Phones in Blatant Disregard to the Fourth Amendment and the Federal Phones Warrant Terms.....	17
B.	The Federal Phones and Computer Warrants Are Unconstitutionally Overbroad and Authorized Seizure of Evidence for Which No Probable Cause Existed	19
C.	The Court Should Hold a Suppression Hearing.....	22
IV.	THE NEW YORK STATE RESIDENCE WARRANT VIOLATED THE FOURTH AMENDMENT; THE GOVERNMENT CANNOT BELATEDLY CURE THOSE CONSTITUTIONAL DEFECTS.....	23
A.	The NY Residence Warrant Purported to Seek Seemingly Anything and Everything from Mr. Daskal’s Residence and Computers	24

B.	The NY Residence Warrant Did not Provide Adequate Guidance Limiting the Executing Authorities’ Discretion	25
C.	The NY Residence Warrant Purported to Authorize Search and Seizure of Materials Exceeding any Probable Cause Showing.....	26
D.	The State Authorities’ Unconstitutional Seizure of Approximately 30 Devices Tainted Any Attempt to Search Selected Devices Later Pursuant to a Federal Warrant	28
V.	THE COURT SHOULD ORDER THE GOVERNMENT TO FILE A BILL OF PARTICULARS TO PROVIDE MR. DASKAL WITH ADEQUATE NOTICE OF THE CHARGES AGAINST HIM.....	31
VI.	CONCLUSION.....	34

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971)	8
<i>In re 650 Fifth Avenue and Related Properties</i> , 934 F.3d 147 (2d Cir. 2019)	22
<i>Riley v. California</i> , 573 U.S. 373 (2014)	12, 19
<i>United States v. Bortnovsky</i> , 820 F.2d 572 (2d Cir. 1987)	32
<i>United States v. Buck</i> , 813 F.2d 588 (2d Cir. 1987)	9, 10
<i>United States v. Cioffi</i> , 668 F. Supp. 2d 385 (E.D.N.Y. 2009)	19, 23, 30, 31
<i>United States v. Clark</i> , 638 F.3d 89 (2d Cir. 2011)	29
<i>United States v. Davis</i> , 906 F.2d 829 (2d Cir. 1990)	5, 7
<i>United States v. Falso</i> , 544 F.3d 124	20
<i>United States v. Gammarano</i> , No. 06-CR-0072, 2007 WL 2077735, (E.D.N.Y. July 18, 2007)	33
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	19, 26
<i>United States v. George</i> , 975 F.2d 72 (2d Cir. 1992)	9, 26
<i>United States v. Gigante</i> , 979 F. Supp. 959 (S.D.N.Y. 1997)	10
<i>United States v. Hernandez</i> , No. 09-CR-625, 2010 WL 26544, (S.D.N.Y. Jan. 6, 2010)	8, 9, 10, 21, 22

<i>United States v. King</i> , No. 21-CR-255, 2022 WL 875383, (S.D.N.Y. Mar. 24, 2022)	10
<i>United States v. LaChance</i> , 788 F.2d 856 (2d Cir. 1986)	25
<i>United States v. Lahey</i> , 967 F. Supp. 2d 698 (S.D.N.Y. 2013)	20
<i>United States v. Liu</i> , 239 F.3d 138 (2d Cir. 2000)	9
<i>United States v. Mandell</i> , 710 F. Supp. 2d 368 (S.D.N.Y. 2010)	32
<i>United States v. Martin</i> , 157 F.3d 46 (2d Cir. 1998)	12
<i>United States v. Matias</i> , 836 F.2d 744 (2d Cir. 1988)	13
<i>United States v. Metter</i> , 860 F. Supp. 2d 205 (E.D.N.Y. 2012)	31
<i>United States v. Nejad</i> , 487 F. Supp. 3d 206 (S.D.N.Y. 2020)	13, 14
<i>United States v. Pinto-Thomaz</i> , 352 F. Supp. 3d 287 (S.D.N.Y. 2018)	30
<i>United States v. Reilly</i> , 76 F.3d 1271 (2d Cir. 1996)	15
<i>United States v. Romain</i> , No. 13-CR-724, 2014 WL 6765831 (RWS)	29
<i>United States v. Rosa</i> , 626 F.3d 56 (2d Cir. 2010)	26
<i>United States v. Siddiqi</i> , No. 06-CR-377, 2007 WL 549420, (S.D.N.Y. Feb. 21, 2007)	33
<i>United States v. Smith</i> , 967 F.3d 198 (2d Cir. 2020)	11, 12
<i>United States v. Trzaska</i> , 111 F.3d 1019 (2d Cir. 1997)	14

<i>United States v. Ulbricht</i> , 858 F.3d 71 (2d Cir. 2017)	19
<i>United States v. Vilar</i> , No. 05-CR-621 (KMK), 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007)	26
<i>United States v. Voustianiouk</i> , 685 F.3d 206 (2d Cir. 2012)	19
<i>United States v. Wagner</i> , 989 F.2d 69 (2d Cir. 1993)	27
<i>United States v. Walsh</i> , 194 F.3d 37 (2d Cir. 1999)	32
<i>United States v. Wey</i> , 256 F. Supp. 3d (S.D.N.Y. 2017)	8, 11, 18, 19, 23, 25, 28
<i>United States v. Winn</i> , 79 F. Supp. 3d 904 (S.D. Ill. 2015)	8, 10
<i>United States v. Zemlyansky</i> , 945 F. Supp. 2d 438 (S.D.N.Y. 2013)	11, 19, 22, 26, 27
<i>United States v. Zucco</i> , 694 F.2d 44 (2d Cir. 1982)	27
<i>Walczyk v. Rio</i> , 496 F.3d 139 (2d Cir. 2007)	22
<i>Wong Sun v. United States</i> , 371 U.S. 471 (1963)	15
Statutes	
18 U.S.C. § 2256(8)	21
18 U.S.C. § 2423	14, 32
U.S. Const. Amend. IV	9

EXHIBIT LIST

Exhibit A
NYPD Enterprise Case Management System
Exhibit B
Kings County Arrest Fax Cover Sheet
Exhibit C
Miranda Warnings
Exhibit D
Letter Faxed to New York City Police Department on May 10, 2018
Exhibit E
September 21, 2020 Court Decision and Order
Exhibit F
United States v. Jacob Daskal Indictment
Exhibit G
April 9, 2021 Government Discovery Letter
Exhibit H
State Search Warrant Application for Jacob Daskal Residence and Devices
Exhibit I
State Search Warrant for Jacob Daskal Residence and Devices
Exhibit J
State Search Warrant Application for Jacob Daskal Devices
Exhibit K
State Search Warrant for Jacob Daskal Devices
Exhibit L
Search Warrant Application for Jacob Daskal Cellular Devices
Exhibit M
Search Warrant for Jacob Daskal Cellular Devices
Exhibit N
Search Warrant Application for Jacob Daskal Computers

Exhibit O
Search Warrant for Jacob Daskal Computers
Exhibit P
Transcript of Kings County Case Dismissal on April 23, 2021
Exhibit Q
Transcript of Conference on August 12, 2020
Exhibit R
Transcript of Court Appearance on September 23, 2019
Exhibit S
Email Correspondence with AUSA Erin Reid from May 23, 2022
Exhibit T
Property Transmittal (Devices)

We respectfully submit defendant Jacob Daskal's amended memorandum of law in support of his omnibus pretrial motions requesting that the Court: (1) suppress the fruits of the searches of his cellular telephones; (2) suppress the fruits of the searches of Mr. Daskal's computers; (3) suppress the fruits of the searches of his home; (4) or, in the alternative, hold a suppression hearing regarding the searches of Mr. Daskal's devices and home; and (5) order the government to file a bill of particulars.

I. PRELIMINARY STATEMENT

Jacob Daskal was first arrested for the alleged sexual misconduct presented in this Indictment on May 10, 2018—more than four years ago. But that arrest did not come at the hands of the United States Attorney's Office for the Eastern District of New York. Mr. Daskal was first arrested by the New York Police Department ("N.Y.P.D."), on a complaint by the Kings County District Attorney's Office.

For more than three years, the Brooklyn D.A.'s Office litigated largely the same charges presented in the federal Indictment filed here. Indeed, the State prosecution suffered several setbacks, including a ruling by the N.Y. State Supreme Court, by Justice Riviezzo, suppressing all evidence obtained from the search of two smartphone mobile devices seized from Mr. Daskal's residence pursuant to a N.Y. State Court search warrant ("NY Phone Warrant"). Justice Riviezzo found that the warrant suffered from Fourth Amendment defects because it authorized overbroad seizures of items, based on a much narrower probable cause showing in the warrant's supporting affidavit, and lacked particularity for the searching officers, resulting in a quintessential unlawful general search of Mr. Daskal's phones.

Only after confronting this setback, did the United States Attorney's Office take over this prosecution. Thus, more than three years after his initial arrest at the hands of the N.Y.P.D., Mr.

Daskal was arrested a second time, in February 2021, this time by federal authorities. He was indicted on three counts of Mann Act violations, all involving allegations of sexual misconduct with a single minor female. The charges vary only based on time and travel with the alleged victim. The charges themselves are not complicated ones and involve largely the testimony of a single witness, who the government seeks to corroborate through various electronic communications and technological location data. Because this corroboration is critical to the government's case, their searches were the most important law enforcement work conducted here. Regrettably, that work was tainted by sloppy presentation of search warrants by State officials, which necessarily poisoned the subsequent, and unnecessarily delayed, federal warrants.

The motions below reveal the unconstitutional actions that resulted in broad, intrusive and indefensible general searches of Mr. Daskal's most private belongings—his private communications, thoughts, feelings, business transactions, medical conditions, family events and crises, and much more.

This case is unusual because we do not write on a clean slate about these constitutional infirmities. The Court need not rely on our arguments alone. Another judge, from the New York State Supreme Court, already has found at least one of these warrants—the NY Phone Warrant—unconstitutional. It, therefore, is far from coincidence that this Court is now presiding over these charges, years after the New York State Court had been dealing with them. The government seeks a “do-over” on its searches of Mr. Daskal's private belongings. We urge below, based on constitutional requirements, that it should not be given one.

This Court should suppress the evidence already ordered suppressed by N.Y. Supreme Court Justice Riviezzo, find the subsequent federal warrants to be tainted as fruit of the poisonous tree and defective in their own form, and further find that the other N.Y. State warrant ordering

the search of Mr. Daskal's home, was likewise unconstitutional—it lacked probable cause for the seizures it purported to authorize, failed to particularize the searches permitted, and prompted broad seizures of devices and materials from Mr. Daskal's home.

Simply because the allegations here are sordid, the government is not given a pass to ignore the Constitution and federal law. Indeed, our fealty to the Constitution is tested most in these types of cases. We are challenged here not to overlook the law because of the nature of the charged crime. If we fail, we become a country not governed by the rule of law, but one that condemns our citizens based on emotional passion and reaction.

We respectfully urge this Court to suppress evidence seized based on New York State and federal law enforcement's violations of the United States Constitution.

II. THE SEARCHES OF MR. DASKAL'S PHONES ARE INDELLIBLY TAINTED BY THE STATE AUTHORITIES' PRIOR UNCONSTITUTIONAL SEARCH, REQUIRING SUPPRESSION OF ALL FRUITS OF THOSE SEARCHES

Two mobile smartphones were seized from Mr. Daskal upon his arrest on N.Y. State court charges on May 10, 2018. A New York State Court warrant was not issued for the search of these phones until October 10, 2018 (hereinafter, the "NY Phones Warrant"). There was no reason given for this five-month delay. Later, by Order of the New York State Supreme Court, dated September 21, 2020, this Warrant was found to be unconstitutional, in violation of the Fourth Amendment's proscription against general warrants. (Ex. E at 5-6.) After this suppression order, the federal government formally stepped in, arresting Mr. Daskal in February 2021 on the same alleged conduct as the Kings County prosecution.

Upon production of discovery in this case, the defense first learned that federal prosecutors obtained a second warrant for the contents of Mr. Daskal's smartphones on February 19, 2019 (hereinafter, the "Federal Phones Warrant"). Before obtaining its own warrant, however, federal law enforcement had already received information from N.Y.P.D. and state law enforcement

authorities that was extracted from earlier searches of these same phones based on the unconstitutional N.Y. Phones Warrant. Thus, “fruits” from subsequent searches under the Federal Phones Warrant are tainted and must be suppressed. Alternatively, the Federal Phones Warrant is also unconstitutionally overbroad and lacked particularity, giving little to no direction to federal agents conducting the later searches.

A. The New York State Supreme Court Found the NY Phones Warrant Unconstitutionally Overbroad and Lacking Particularity

The New York Supreme Court’s Order suppressing evidence seized pursuant to the NY Phones Warrant is clear and persuasive. (Ex. E.) Justice Riviezzo held that the Warrant was unconstitutional as it:

allows for a search of every aspect of the phone – GPS, voice messages, call history, contact information, photos, videos, calendar contents, social media communications etc., with ***no limit by date*** that the complainant knew or was in contact with the defendant or alternatively ***without a limit by the content*** or method by which the complainant alleges she communicated with the defendant.

(*Id.* at 5) (emphasis added). The categories of items to be seized from Mr. Daskal’s cellphones literally “allowed for a search of every aspect of the phone[s] . . .” (*Id.*) The Court contrasted the limitless language in the NY Phones Warrant to an earlier issued Warrant for Daskal’s Home – requested by the same Kings County prosecutor – which had some narrower categories.¹ The N.Y. Court reasoned that “at the very least, the warrant should have contained similar limiting language as in the warrant for his residence and computers, such as “records of communication between the subject and the witness.” (*Id.* at 6.)

¹ This narrower category still cannot salvage the New York State warrant for Mr. Daskal’s home which suffered from overbreadth and lack of particularity, prompting significant over-seizure of materials and devices. *See infra* § IV.

Thus, the N.Y. Supreme Court held the NY Phones Warrant to be unconstitutionally overbroad and lacking in particularity to guide searching officers, warranting suppression of “any and all evidence seized from the cellular telephones.” (*Id.* at 6.)

B. The Government Should Be Collaterally Estopped from Contesting the State Court’s Suppression Order

To determine whether to give collateral estoppel effect to a state suppression order, the Second Circuit has directed that “the pivotal question is whether there was a close or significant relationship between the federal and New York State prosecutors during the local suppression hearing or whether the federal authorities controlled or actively participated in that hearing such that their interests in enforcing federal law were sufficiently represented.” *United States v. Davis*, 906 F.2d 829, 834 (2d Cir. 1990) (internal quotation marks omitted). The Court avoided defining the contours of that relationship because the circumstances in that case “f[e]ll far short of showing the kind of close relationship that would meet even the lower hurdle of active participation.” *Id.* at 835.

The facts here leave no doubt that federal prosecutors were already heavily involved in this investigation and prosecution of Mr. Daskal long before the suppression litigation before Justice Riviezzo.

First, the federal investigation dates back, at least, to early 2019 (Ex. Q), which far predated the motions litigation and state court suppression order. (Ex. E.) At an August 12, 2020, conference in Mr. Daskal’s New York case, the state prosecutor advised the court that “I had said this first in court *on February 11, 2019*, that the federal government is – intends to take the case.” (Ex. Q at 3) (emphasis added). According to the local prosecutor, federal officials interviewed the complainant “shortly before then” in January 2019. (*Id.*) At that point in time, federal authorities already had conferred with New York law enforcement and had “taken a large amount of the

electronic evidence that was recovered in the [New York] search warrant.” (*Id.*) The Brooklyn prosecutor, Assistant District Attorney (“ADA”) O’Donnell, expressed uncertainty as to whether federal prosecutors obtained a separate search warrant for the content of the Daskal Phones, which already had been searched by NYPD and materials downloaded for use by federal authorities. (*Id.*)

According to ADA O’Donnell’s affidavit in opposition to Mr. Daskal’s motion to suppress evidence from the New York searches, his Office delivered two phones – a “Samsung Galaxy S8” and “Apple Iphone” – ***and a “500GB Western Digital Portable Hard drive” to the FBI*** on or about November 27, 2018. (Ex. T at 1) (emphasis added.) This hard drive undoubtedly contained the NYPD’s digital extractions from the phones based on the NY Phones Warrant in October 2018.

Thus, after Mr. Daskal’s initial New York arrest in May 2018, local Kings County prosecutors obtained the NY Phones Warrant in October 2018, executed that Warrant, uploaded the extractions from the searches onto a hard drive, and in the following month (November 27, 2018), turned over the two phones and extractions to federal authorities. Indeed, in the Affidavit² in Support of the Federal Phones Warrant, Ex. L, the FBI Agent conceded receipt “of the forensic extractions [that the Brooklyn District Attorney’s Office] have conducted of them.” (Ex. L ¶ 14 at 8).

Less than two months later, in January 2019, federal prosecutors interviewed the state court complainant for the first time, presumably after reviewing the New York State produced material. (Ex. Q at 3). While the FBI Affiant in support of the Federal Phones Warrant indicated

² The FBI Affiant’s name is redacted in the copy of the Affidavit provided to the defense in discovery. We ask that the Court order the government to reveal the identity of the FBI Affiant, as this information may become relevant, and inevitably public, if the Court grants an evidentiary hearing. Moreover, the defense should be able to review the reported disciplinary record of the affiant, if applicable, to challenge the credibility of the information reported, or if later government disclosures suggest the need for a *Franks* hearing.

that “the FBI ha[d] not searched either of the SUBJECT PHONES,” prior to applying for the Federal Phones Warrant, s/he remained conspicuously silent as to what was done with the received “forensic extractions” “conducted” by the Brooklyn District Attorney’s Office. (Ex. L, para. 14, at 8). This omission in the same paragraph where the FBI Agent stated under oath that no searches were conducted of the phones raises the question of what the FBI did with the State court “extractions.” If these were not searched as well, it is presumed the agent would have included this fact when affirming what the agents did not review before seeking the Federal Warrant.

Thus, there is at least a *prima facie* basis to believe that Federal and State authorities reviewed the **same** New York State search warrant returns from the Daskal Phones, which later became the subject of the New York State Court suppression motion almost two years later. No federal charges were brought before the September 21, 2020 suppression order from N.Y. Supreme Court. Federal prosecutors waited for the result of that litigation, and only after the evidence was ordered suppressed by the State Court, did it seek the federal indictment here.

Given this timeline, which unequivocally shows federal prosecutors’ involvement in the Daskal investigation and State prosecution from as early as **November 2018**—approximately 27 months before Mr. Daskal’s federal arrest—it is clear there was a “close or substantial relationship” between federal and state prosecutors at the time of the New York suppression litigation in the summer and early fall of 2020. *Davis*, 906 F.2d at 834. Thus, this Court should give collateral estoppel effect to the State Court Order, finding the NY Phones Warrant to be unconstitutional.

Alternatively, a hearing is necessary to determine the full extent that federal prosecutors actively aided the state prosecutors during the State court proceedings.

C. Alternatively, This Court Should Independently Find the NY Phones Warrant Constituted an Unconstitutional “General Warrant” in Violation of the Fourth Amendment, Requiring Suppression of All Evidence Seized From the Phones

Regardless of the *Davis* test, this Court should independently find that the NY Phones Warrant violated the Fourth Amendment as it is both unconstitutionally overbroad and lacks particularity to focus the searches of executing law enforcement officers.

1. The NY Phones Warrant Was Overbroad

As the New York State Court found, the NY Phones Warrant authorized the wholesale seizure of unlimited categories of items from Mr. Daskal’s two cellphones. This made the warrant, in effect, an unconstitutional “general warrant.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Indeed, the Warrant authorized nothing less than a wholesale seizure of all parts of Mr. Daskal’s private life memorialized in the phones—“any and all” voice messages, text messages, call history, contacts, video and photograph images, calendar contents, social media interactions, web browsing history, and more (Ex. K at 1)—regardless of whether they were linked to the complainant’s allegations or to any crime. *See e.g., United States v. Hernandez*, No. 09-CR-625, 2010 WL 26544, *8 (S.D.N.Y. Jan. 6, 2010) (search warrant that authorizes the seizure of items as to which there is no probable cause is impermissibly overbroad). The NY Phones Warrant did not even attempt to connect the items authorized to be seized with the probable cause showing in the supporting affidavit, effectively untethering it to any established probable cause. *See United States v. Wey*, 256 F. Supp. 3d 355, 382 (S.D.N.Y. 2017).

The district court in *United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015), confronted a similarly worded warrant for the search of contents of a smartphone. There, “[t]he warrant authorized the seizure of ‘any or all files’ contained on the cell phone and its memory card” constituting evidence of a public indecency offense, “including, but not limited to, the calendar,

phonebook, contacts, SMS messages, MMS messages, emails, pictures, videos, images, ringtones, audio files, all call logs, installed application data, GPS information, WIFI information, internet history and usage, any system files, and any deleted data.” *Id.* at 919. Problematically “with the description of the object of the search — ‘any or all files’ — is that the police did not have probable cause to believe that everything on the phone was evidence of the crime of public indecency. *Id.* The court denounced the template-nature of the search warrant’s list, finding “[t]his particular template authorized the seizure of virtually every piece of data that could conceivably be found on the phone.” *Id.* As a result, the *Winn* court held that the “the warrant was facially overbroad” because objects of the search exceeded the probable cause to support it and was not as particular as the circumstances would allow. *Id.*; see also *United States v. Buck*, 813 F.2d 588, 591 (2d Cir.1987) (finding impermissibly broad a warrant rife with “general boilerplate terms, without either explicit or implicit limitation on the scope of the search”).

Mr. Daskal’s case is functionally equivalent to *Wey*, *Hernandez*, and *Winn*. The lack of narrowing language in the items to be seized in the NY Phones Warrant authorized the seizure of virtually every piece of data that could conceivably be found in the two smartphones. Under these circumstances, the appropriate remedy is suppression of all items seized.

2. The NY Phones Warrant Lacked Particularity

A search warrant must state with particularity “the place to be searched, and the persons or things to be seized.” U.S. Const. Amend. IV. A warrant is sufficiently particular only if it “enable[s] the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize.” *United States v. George*, 975 F. 2d 72, 75 (2d Cir. 1992); accord *United States v. Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (“A warrant must be sufficiently specific to permit the rational exercise of judgment [by the executing officers] in selecting what items to seize.”) (quotations omitted). As little as is possible should be “left to the

discretion of the officer executing the warrant.” *Buck*, 813 F.2d at 590-91. The NY Phones Warrant did not meet this requirement either.

At best, the supporting affidavit provided probable cause to seize materials from August 2017 to November 2017 relating to Mr. Daskal’s communications with the complainant, as well as any images or videos. Instead of limiting the searches accordingly, the NY Phones Warrant sought data content from the Phones without circumscribing the relevant person, timeframe, or subject matter sought. (*See* Ex. K). Absent such limitations, the warrant is insufficiently particular. *See United States v. Gigante*, 979 F. Supp. 959, 966–67 (S.D.N.Y.1997); *Hernandez*, 2010 WL 26544, at *11; *United States v. King*, No. 21-CR-255 (NSR), 2022 WL 875383, at *4 (S.D.N.Y. Mar. 24, 2022).

The NY Phones Warrant merely described the categories of data that reside in *every* phone, rather than particular items, *e.g.*, names of individuals texting, the telephone numbers used to text, when the texts occurred. This is insufficiently particular. *Hernandez*, 2010 WL 26544, at *10 (the categories of items to be seized from a business lack particularity where they “could have encompassed most all of the business records on the premises”); *see also Winn*, 79 F. Supp. 3d at 919 (“With respect to the categories of data for which the police did have probable cause—the photos and the videos—the warrant was not as particular as could be reasonably expected given the nature of the crime and the information the police possessed”).

Lastly, while the NY Phones Warrant listed the statutes under investigation, any relevant factual context to guide the agents is completely absent. (*See* Ex. K). The Warrant did not name specific individuals, places, timeframes, or any contextual allegations discussed in the underlying supporting affidavit. The general penal law statutes cited in the Warrant, without more, cannot effectively curtail the executing officers’ discretion and limit the searches and seizures to materials

subject to probable cause. That too fails the Fourth Amendment’s particularity requirement. *See Wey*, 256 F.Supp.3d at 386 (“By the Warrants’ terms, then, no connection to any suspected crime or to any other individual or entity . . . is necessary to render the expansive list of items set forth in Exhibit A seizable.”); *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 454 (S.D.N.Y. 2013) (warrant violated Fourth Amendment as “[a]t no point prior to or during the enumeration of these eight items does the warrant offer any indication of the relevant criminal allegations.”).

D. The Unreasonable Five-Month Delay Between Seizure and Warrant Also Requires Suppression Under *Smith*

NYPD seized Mr. Daskal’s smartphones on May 10, 2018, incident to his arrest. (Ex. J at ¶ 10.) The Kings County prosecutor did not seek a search warrant until October 10, 2018. (Ex. J.) This delay of *five months* between seizure and search warrant application was unjustified. Nothing happened in the interim, between arrest and the drafting of the warrant application. This delay was unreasonable and, by itself, warrants suppression pursuant to the test set forth in *United States v. Smith*, 967 F.3d 198, 206 (2d Cir. 2020).

The Second Circuit held in *Smith* held that a 31-day delay was unreasonable and ordered suppression. *Id.* at 202. The Court created a four-factor test to determine whether delay requires suppression:

[T]he following four factors are generally relevant to whether the police have waited an unreasonable amount of time before seeking a search warrant: (1) the length of the delay, (2) the importance of the seized property to the defendant, (3) whether the defendant had a reduced property interest in the seized item, and (4) the strength of the state’s justification for the delay.

Id. at 206. The *Smith* Court explained that it is common for law enforcement to temporarily seize a device if probable cause existed. *Id.* at 202. However, it also noted that “the Fourth Amendment requires that they act with diligence to apply for a search warrant.” *Id.* Seizures based upon

probable cause will become unconstitutional “if police act with unreasonable delay in securing a warrant.” *Id.* (quoting *United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998)).

Here, the five-month delay is five times longer than the one-month delay in *Smith*, which the Court found to have “well exceed[ed] what is ordinarily reasonable.” 967 F.3d at 206. The Daskal Phones were “smartphones,” and important to Mr. Daskal’s daily life, as evidenced by his personal possession of them at the time of his State arrest. (Ex. J at ¶¶ 9-10.) The fact that these were “smartphones” is “vital,” according to *Smith*, given the “fundamental distinction between one’s ordinary personal effects and one’s personal electronic devices.” 967 F.3d at 207 (citing *Riley v. California*, 573 U.S. 373 (2014)). Although the government had its own law enforcement interest in the smartphones, that interest became more limited as the delay grew longer. *Smith*, 967 F.3d at 209. Nowhere in the underlying affidavit does the Kings County prosecutor explain the five-month delay. (Ex. J.) However, the time needed to prepare the affidavit was minimal given its similarity to the affidavit in support of the Home Warrant, which was prepared the same day of Mr. Daskal’s arrest. (Compare Exs. H and J.) Indeed, strangely, the affidavit in support of the NY Phones Warrant is typed with the arrest date, indicating “May 10, 2018.” (Ex. J, at 4.) However, the month of “May” is crossed out, and written over by hand with “October.” (*Id.*) Apparently, the entire affidavit might have been prepared timely, on the date of Mr. Daskal’s arrest, but the prosecutor inexcusably sat on it, not presenting it to the court for purposes of obtaining the Warrant, until five months passed. No justification was given for this lengthy delay.

Pursuant to *Smith*, the government’s five-month delay was inexcusable and unreasonable, independently warranting suppression.

E. The Subsequent Federal Phones Warrant Relied Upon Tainted Evidence, and Therefore Cannot Be Relied Upon to Provide the Lawful Basis to Avoid Suppression of Seized Evidence From the Daskal Phones

The relevant timeline of the ongoing seizure of Mr. Daskal's smartphones reveals why the government cannot rely on the later Federal Phones Warrant to save them from suppression. Mr. Daskal's phones were seized on May 10, 2018 (incredibly, now more than four years ago); no warrant of any kind was issued until October 10, 2018, when the NY Phones Warrant was ordered; this Warrant was later deemed unconstitutional by the New York Supreme Court in Kings County (Ex. E); the FBI received the Daskal Phones and their unlawfully seized N.Y. State extractions in November 2018 (*see* Ex. T); federal law enforcement and prosecutors presumably used the N.Y. State forensic extractions of the phones in preparing for an interview they conducted of the complainant in January 2019; and only after the production of the New York State materials did federal prosecutors seek a federal warrant in February 2019 to search and seize contents of the Phones for alleged federal crimes.

Thus, federal law enforcement apparently reviewed material gathered in response to the NY Phones Warrant in aid of its own interviews, and to further investigate federal crimes *before* they obtained the Federal Phones Warrant. As Judge Nathan reasoned in *United States v. Nejad*, upon analyzing the same kind of overlap between State and Federal law enforcement searches from a single State Court search warrant: "This conduct was likely unconstitutional because review of search-warrant returns must be done in conformity with the warrants themselves." *United States v. Nejad*, 487 F. Supp. 3d 206, 210-11 (S.D.N.Y. 2020) (citing *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) ("A search warrant must be confined to the terms and limitations of the warrant authorizing it.")).

In other words, because the NY Phones Warrant only authorized searches for material pertinent to violations of State law (*see* Ex. K: "Rape in the Third Degree (P.L. § 130.40(2)),

Criminal Sexual Act in the Third Degree (P.L. § 130.40(2)), Endangering the Welfare of a Child (P.L. § 260.10(1))”, any review by federal agents for crimes alleged in this Indictment, *i.e.*, the Mann Act and Transportation of Minors, 18 U.S.C. § 2423, would be outside the scope of the authorized searches in the NY Phones Warrant. *See Nejad*, 487 F. Supp. 3d at 209-11 (in reviewing late disclosures by the government about the conduct of searching FBI agents, Court found in *dicta* that it likely would have suppressed evidence had it known that the FBI searched “raw” state court search warrant returns for federal crimes without a federal warrant, because these searches exceeded authority under State court warrant).

Of course, there remains an even broader issue of taint, beyond the issue of whether federal authorities reviewed the “raw” NY Phones Warrant returns to investigate federal crimes outside the express terms of the NY Warrant. There is also the issue that any review of State “forensic extractions,” (Ex. L at 8), performed by federal agents or prosecutors, would lead to unconstitutional taint of the Federal Phones Warrant, such that it could not save the NY Phones Warrant returns. *See United States v. Trzaska*, 111 F.3d 1019, 1026 (2d Cir. 1997) (“[e]vidence seized during an illegal search should not be included in a [search] warrant affidavit”).

Here, the Court can draw a rational inference from the timeline of federal law enforcement involvement that federal authorities used the New York “forensic extractions” it received in November 2018 to prepare for its interview of the complainant in January 2019, and to develop leads that formed the basis of its questioning of the complainant. The complainant’s answers to questions premised on information obtained from the federal review of the State “forensic extractions” created the basis of probable cause in the underlying Affidavit in support of the Federal Phones Warrant in February 2019. Because the agent’s questioning of the complainant was premised on tainted State Court evidence—both because federal authorities could not review

these raw returns to investigate federal crimes and because these returns themselves were based on an unconstitutional general warrant—a neutral magistrate court could not rely on this evidence in making the probable cause assessment for the warrant. *See United States v. Reilly*, 76 F.3d 1271, 1282 n.2 (2d Cir. 1996) (where a warrant is predicated on illegally obtained evidence, the reviewing court must “excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant”).

The Federal Phones Warrant thus cannot save the unconstitutional general NY Phones Warrant because it was impermissibly tainted by it. *See generally Wong Sun v. United States*, 371 U.S. 471 (1963) (“fruits of the poisonous tree,” including leads or connecting proof, should be suppressed under the exclusionary rule).

III. THE COURT SHOULD SUPPRESS THE FRUITS OF THE SEARCHES ON MR. DASKAL’S PHONES AND COMPUTERS: THE FEDERAL WARRANTS WERE OVERBROAD AND THE AGENTS HELD THE DEVICES AND FAILED TO CONDUCT TIMELY RESPONSIVENESS REVIEWS

After Mr. Daskal’s arrest in May 2018, the Kings County District Attorney’s Office immediately got the U.S.A.O./E.D.N.Y. involved in the criminal investigation. In November 2018, they sent the FBI the two smartphones the NYPD seized from Mr. Daskal upon his arrest, as well as a “forensics extraction” of the phones. (Ex. T.) In August 2019, they sent two computers seized from the Daskal Residence under the NY Residence Warrant (*see infra* § IV). (Ex. T.) Each time that the federal government obtained new pieces of electronic evidence from the NYPD, it moved to obtain new warrants, seeking to remove the obvious taint from the unconstitutional general warrants earlier issued by the New York State courts.

Two warrants were issued by Magistrate Judges in the E.D.N.Y.: (1) the Federal Phones Warrant (discussed *supra*) on February 19, 2019 (Ex. M); and (2) a warrant to search the contents of a desktop and laptop computer, earlier seized during the NYPD’s search of Mr. Daskal’s

residence. This second federal warrant was issued on September 26, 2019 (hereinafter, the “Federal Computers Warrant”).

These two federal warrants were identical in the searches that they authorized. Each authorized the search of 22 broad categories of electronic storage items, mostly focused on searching for and seizing child pornography criminal conduct. The affidavits supporting the warrants were also largely identical—indeed except for minor word changes involving the differences between phones and computers, the agent just cut-and-pasted from his earlier affidavit in support of the Federal Phones Warrant, and added very little to the latter Federal Computers Warrant (despite the passage of seven months between warrant dates). (*Compare* Ex. L *with* Ex. N.)

As argued below, the Federal Phones and Computer Warrants were never executed under the terms of the Warrants; responsive materials limited to the Warrants’ terms were never culled from the raw data returns and never “promptly” presented to the Duty Magistrate. The government obviously believes it can run searches whenever and however it wants, giving no mind to the Fourth Amendment.

These Federal Warrants also remained overbroad, focusing on criminal conduct—the possession, production, transmission or purchase and sale of child pornography—that was never mentioned in the underlying affidavits to the warrants, other than reproducing the statutory definition of “child pornography.” The affidavits never connected Mr. Daskal to this broader criminal conduct, let alone the places sought to be searched.

For these reasons, detailed below, this Court should suppress the returns from the Federal Warrants, independent of the taint created by the New York general warrants.

A. The Government Conducted Continuous Searches of the Daskal Phones in Blatant Disregard to the Fourth Amendment and the Federal Phones Warrant Terms

In the evening of February 19, 2019, Magistrate Judge Kuo issued the Federal Phones Warrant to search the contents of Mr. Daskal's two smartphones, which had been taken from him almost a year earlier upon his New York arrest. On the evening of September 26, 2019, Magistrate Judge Levy issued the Federal Computers Warrant to search the contents of two computers taken from Mr. Daskal's residence by the NYPD in May 2018.

The Federal Phones and Computer Warrants, included the same Attachment B (Ex. L at 23 and Ex. O at 4), identifying 22 items to be searched on the subject devices, of which 19 of the 22, directed the agents to focus on child pornography possession, production, transmission or communications. (*Id.*) Only the first two items in the Attachment B involved the specific complainant. Indeed, these two items are the only items for which probable cause appeared to be met in the agent's underlying affidavit supporting the Warrants.

However, it appears the government did not even limit their searches to this overbroad list. As of this date, the government still has not produced its "pertinent" or "responsive" set of warrant returns under the Federal Phones and Computer Warrants. Based on the express terms of those Warrants, the two Magistrate Judges ordered: "[t]he officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and *promptly* return this warrant and inventory to the Duty Magistrate Judge." (Exs. M and O) (emphasis added). Not only has this inventory list presumably not been provided to the Duty Magistrates, no inventory of responsive returns under the Warrants have been produced to defense counsel either. Instead, it appears that the government has not yet conducted its searches under the Warrants' limitations (and, more importantly, the Fourth Amendment's requirements), and

instead has effectively seized the entire contents of Mr. Daskal's smartphones and two computers over the last three years.

In discovery to date, the government has produced to defense counsel only the forensic extractions of the complete electronic devices: (1) Apple iPhone 7; (2) Samsung Galaxy S8; (3) a Dell Desktop Computer; and (4) a Dell Laptop Computer. That is, we only have the **total** content of the phones and computers as extracted using forensic software. This includes, for example, over 105,000 pages of data from the Apple iPhone 7, including business, personal, family, medical and other private matters having nothing whatever to do with the four months of alleged misconduct with the complainant. In other words, the executing agents have treated the Federal Phones and Computer Warrants as a general warrant, giving them full breadth to search the entire contents of Mr. Daskal's most private things at any time they want, searching any parts of the phones or computers they want, using whatever search tools they want. In doing so, the government acts as if there is no Fourth Amendment at all.

It appears the government does not intend to conduct responsiveness reviews at all, and instead seeks to retain the ability to run searches at its whim, or when it deems it must for trial. This runs counter to the Fourth Amendment and interpretive case law by the Second Circuit. Under the Fourth Amendment, the government must complete its responsiveness review "within a 'reasonable' period of time." *Wey*, 256 F. Supp. 3d at 383. We are now more than **three years** removed from the date when the Federal Phones and Computer Warrants were first issued. This is not within the reasonable period of time contemplated in *Wey*. Not even close.

The government has acted as if it could do with these personal electronic devices as they wish. This is not what the Fourth Amendment authorizes. It is also inconceivable that the government could act so flagrantly in disregard to its constitutional obligations with respect to the

most private of possessions of its citizens. People today conduct their business and personal affairs largely electronically. The ability to seize and search such a vast, interconnected and personal cache of data, if not restricted to particularized items for which probable cause is shown, amounts to a prohibited general warrant. *See Riley*, 573 U.S. at 402 (finding seizure and search of a person’s cellphone equivalent to “ransacking his house for everything which may incriminate him”); *See United States v. Cioffi*, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009) (“The dawn of the Information Age has only heightened . . . [privacy] concerns. The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because [c]omputers . . . often contain significant intermingling of relevant documents with documents the government has no probable cause to seize.”).

Here, the government’s strategy of continuing to hold and search the entirety of Mr. Daskal’s personal, virtual “house” for as long as the agents want or need, without regard to the terms of the Federal Phones and Computer Warrants or the Fourth Amendment, amounts to a general warrant. *See Wey*, 356 F. Supp. 3d at 386-87; *United States v. Ulbricht*, 858 F.3d 71, 99-100 (2d Cir. 2017) (quoting *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013)). Suppression is required. *See, e.g., United States v. Voustianiouk*, 685 F.3d 206, 212 (2d Cir. 2012).

B. The Federal Phones and Computer Warrants Are Unconstitutionally Overbroad and Authorized Seizure of Evidence for Which No Probable Cause Existed

The Court should also independently suppress evidence seized from Mr. Daskal’s Phones and Computers because the Federal Warrants, while a bit more restrained than the NY Warrants, remained unconstitutionally overbroad. As stated above, the Fourth Amendment prohibits overly broad warrants. “In determining whether a warrant is overbroad, courts must focus on whether there is probable cause to support the breadth of the search that was authorized.” *Zemlyansky*, 945 F. Supp. 2d at 464 (quotation and citation omitted).

The Federal Phones and Computer Warrants were overbroad because they allowed the government to seize 20 different items that focused on the production, possession, transmission, purchase and sale and other transactions related to child pornography, without *any* presentation of evidence that could lead the Magistrate Judge to find probable cause to connect Mr. Daskal's contents of his phones and computers to this criminal conduct. (See Ex. L, Attach. B, at 23-26; Ex. O, Attach. B, at 4-7.) Indeed, the government appears to rely solely on speculation that because it had a single complainant, who presented testimony of sexual abuse, then Mr. Daskal must be committing child pornography-related crimes.³ Of course, while the probable cause threshold remains relatively low, it does not authorize searches based on speculation alone. See *United States v. Lahey*, 967 F. Supp. 2d 698, 727 (S.D.N.Y. 2013) (granting suppression where warrant was not supported by probable cause because it was “premised on very thin evidence connecting [defendant] (let alone [the place to be searched]), to the [alleged criminal conduct].”) Indeed, in even the flimsiest probable cause showings, the government sometimes adds boilerplate language that attempts to bootstrap abuse of one alleged victim to a larger pattern of behavior, by adding language from an “expert” witness agent who avers that she has seen this pattern of behavior in her experience of investigating these types of crimes. *But see United States v. Falso*, 544 F.3d at 124 (finding search warrant unsupported by probable cause when affidavit contained only speculative statement that defendant may have engaged in certain criminal conduct and generalized conclusions about the habits of other individuals likely to engage in the charged

³ While the government may retort that some of the depictions sought to be searched in these 20 broad categories of items could be of the complainant herself, this argument would not pass constitutional muster. None of these 20 categories of item refer specifically to the complainant, while Item 2 of Attachment B does. (Exs. L and O, Item 2: “All images, motion pictures, films, videos and other recordings of the Victim.”) The Warrants’ overbroad search authorizations swallow up the two narrow items—the only ones—that connect the searches to the complainant.

conduct, but affirming denial of suppression on good faith exception grounds). However, in this case, even this specious language is missing in the affidavits here.

Indeed, the only mention of child pornography in the underlying affidavit is under a section called “Technical Terms,” where the definition of “child pornography” is provided, as it is defined in 18 U.S.C. § 2256(8). (Ex. L, at 9, and Ex. N, at 10.) But there is no factual link to explain why it is being defined, and no attempt to connect Mr. Daskal to conduct related to child pornography transactions, let alone that such fruits or instrumentalities might be found in the place sought to be searched.

The only items in the Federal Warrants connected to the complaining witness are the first two or three listed in the Warrant. (*See* Ex. L, Attach. B, at 23; Ex. O, Attach. B, at 4.) Most if not all (except for the technical items which seek computer-specific identifications) of the remaining 19 items authorize broad categories of searches linked to child pornography criminal conduct.⁴

In determining whether a warrant is overbroad, courts focus on whether probable cause exists “to support the breadth of the search that was authorized.” *Hernandez*, 2010 WL 26544, at

⁴ Attachment B to the Warrants includes the following categories directed at child pornography-related criminal conduct or engaging in the business of child pornography: “images of child pornography” (Item 4); “motion pictures, films, videos, and other recordings of visual depictions of minors” (Item 5); material “bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce” of child pornography (Item 6); “[a]ddress books, mailing lists, supplier lists, mailing address labels . . . in connection with the purchase, sale, trade, or transmission of any visual depiction of minors engaged in sexually explicit conduct” (Item 9); all records “reflecting personal contact and other activities with individuals believed to be minors” (Item 11); “any and all records . . . concern[ing] any Internet accounts used to possess, receive, or distribute child pornography” (Item 13); “User attribution information (i.e. files and other data such as chats or e-mails) relevant to the trading of child pornography” (Item 14); “records of Internet Protocol addresses used; records of Internet activity,” “all of which constitute evidence, fruits and instrumentalities” of violations including trafficking or engaging in enterprises that traffic in child pornography (Item 22).

*8 (citations omitted). Probable cause is demonstrated where the “totality of circumstances indicates a ‘fair possibility that contraband or evidence of a crime will be found in a particular place.’” *Walczyk v. Rio*, 496 F.3d 139, 156 (2d Cir. 2007) (citations omitted). A warrant permitting “fairly broad” seizure of materials is permitted *only* where “the affidavit in support of the search warrant application provides the necessary basis for a determination of probable cause to seize items in *each* of those categories.” *Hernandez*, 2010 WL 26544, at *8 (emphasis added); *accord Zemlyansky*, 945 F. Supp. 2d at 453. This is not the case here.

There was no *attempt* in the Agent’s underlying affidavit to connect Mr. Daskal with the broad 19 categories of child pornography-related crimes, let alone the places to be searched. Nothing at all. The absence of any attempt to connect Mr. Daskal with this criminal conduct renders these categories of items constitutionally infirm. And because these items utterly dominate the amount and breadth of searches authorized by the Federal Phones and Computer Warrants, the Warrant cannot stand constitutional scrutiny. This, in combination with the fact that the execution of these Warrants renders them lawless general warrants, should require suppression of all evidence seized from the Daskal phones and computers. *See In re 650 Fifth Avenue*, 934 F.3d 147, 164 (2d Cir. 2019) (“Under all these circumstances, the Government’s reliance on this warrant was not ‘objectively reasonable.’”).

C. The Court Should Hold a Suppression Hearing

To resolve issues related to whether the federal agents received “tainted” information or fruits from the NY Phones Warrant and the execution of the Federal Phones and Computer Warrants, the Court should hold a suppression hearing. Issues that the Court may need to resolve at a hearing include: (1) the use of the NYPD “forensic extractions” of the Daskal Phones; (2) the government’s execution of the Federal Phones and Computer Warrants; (3) why no responsiveness determinations were made during the searches conducted by federal agents; (4) identification of

the full set of searches conducted by federal agents and/or NYPD officers and timing of these searches; and (5) the government's reasons for not disclosing any responsiveness reviews under the Federal Warrants.

Unless the government can satisfactorily show that its reviews of the contents of the Daskal Phones were not tainted by the NY Phones Warrant extractions; that the contents of the Phones and Computers were searched promptly, not continuously, and under the limited terms of the Federal Phones and Computer Warrants; and that no subsequent searches were conducted outside a reasonable timeframe permitted by the Fourth Amendment, as interpreted by *Wey*, the phone and computer evidence must be suppressed.

IV. THE NEW YORK STATE RESIDENCE WARRANT VIOLATED THE FOURTH AMENDMENT; THE GOVERNMENT CANNOT BELATEDLY CURE THOSE CONSTITUTIONAL DEFECTS

The constitutional missteps plaguing the New York State Residence Warrant (“NY Residence Warrant”) are similarly emblematic of the constitutional problems plaguing the searches of Mr. Daskal’s electronic devices: the state authorities’ execution of an unconstitutional warrant tainted the government’s subsequent efforts to cure the Fourth Amendment violations. The NY Residence Warrant purported to authorize seizure of broad categories of materials and devices for which there was no probable cause. Predictably, the state authorities proceeded to seize vast troves of materials from Mr. Daskal’s residence, *including approximately 30 electronic devices* without probable cause. Over a year later, the federal government attempted to determine which of the 30 devices was potentially subject to probable cause—but it was too late. The devices had been seized without probable cause, and held without a valid warrant for approximately 15 months by the time the federal government attempted a Fourth Amendment do-over with a new warrant. The government cannot, however, simply sweep under the rug the prior Fourth Amendment violations that persisted for over a year. *See Cioffi*, 668 F. Supp. 2d at 398-99 (“No court has ever endorsed

the view that it would allow the government to retroactively cure a Fourth Amendment violation”). The materials and over two dozen devices seized from Mr. Daskal’s residence should thus be suppressed.

A. The NY Residence Warrant Purported to Seek Seemingly Anything and Everything from Mr. Daskal’s Residence and Computers

Like the other warrants, the probable cause showing for the May 10, 2018 warrant application to search Mr. Daskal’s Brooklyn home, and computers found therein, was based on the complainant’s recounting of: (1) sexual incidents allegedly involving Mr. Daskal, (2) a letter regarding the allegations indicating “that whatever activity she and the subject engaged in were part of therapy,” which the complainant allegedly wrote “at [Mr. Daskal’s] request and direction,” (3) “two additional letters,” at least one of which denied any alleged sexual contact between Mr. Daskal and the complainant in Chicago that Mr. Daskal allegedly told the complainant he had “scanned . . . onto his computer,” and (4) the complainant’s memory that Mr. Daskal had “two laptop computers, multiple desktop computers, a scanner and a printer”—although the warrant application did not identify which, if any, of the computers Mr. Daskal allegedly used in connection with his correspondence with the complainant. (Ex. H ¶¶ 4-9.)

On that basis, the NY Residence Warrant sought broad swaths of materials from Mr. Daskal’s home, including: (1) “any and all computers . . . or electronic storage devices;” (2) “any and all cellular telephones, cameras, video recorders . . . and other electronic devices;” (3) “any and all handwritten or typed notes containing computer-related information;” (4) “Evidence of ownership and use of the subject location,” including but not limited to “bank statements, . . . personal papers. . . videotapes and photographs of persons;” (5) “any and all data, information, or images evidencing internet usage history;” and (6) “any and all data, information, or images that evidence ownership or use of the device, including, but not limited to . . . photographs, videos, bank

account documents, bills and invoices . . . text messages, instant messenger messages, letters and stored voicemails.” (Ex. I at 1-2.) With such a broad warrant, the state authorities seized vast troves of materials in executing the search: financial documents, personal correspondence from community leaders and friends, and dozens of devices—in total approximately 30 computers were seized during the search. (*See* Ex. R at 3:14.)

B. The NY Residence Warrant Did not Provide Adequate Guidance Limiting the Executing Authorities’ Discretion

As previously addressed, *see supra* § II.C.1, a warrant must include a “description of the property or objects of the search that is sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting which items to seize.” *United States v. LaChance*, 788 F.2d 856, 874 (2d Cir. 1986) (internal quotation marks omitted).

The broadly-drawn seizure categories in the NY Residence Warrant, permitting seizure of virtually all digital or physical materials found in Mr. Daskal’s home—for example, “all computers,” “all handwritten or typed notes,” and all records of “internet usage history”—are anathema to the Fourth Amendment’s particularity requirement. (Ex. I at 1-2.) They simply provide the executing agents with no guidance at all, instead seemingly providing agents with authority to grab everything, invalidating the warrant for lack of particularity. *See Wey*, 256 F. Supp. 3d at 385 (“warrants are insufficiently particularized” where they “set[] forth expansive categories of often generic items subject to seizure—several of a ‘catch-all’ variety—without, crucially, any linkage to the suspected criminal activity, or indeed any meaningful content-based parameter or other limiting principle.”). The permission to seize “any and all” documents, data and objects seemingly falling into a dozen of the warrant’s broad categories, only compounds the particularity problem. (*See* Ex. I at 1-2.) Precisely such warrants “authorizing the seizure of ‘any or all records’ of a particular type,” “frequently lack particularity” as “they include a general,

catch-all paragraph or provision.” *United States v. Vilar*, 05-CR-621 (KMK), 2007 WL 1075041, at *22 (S.D.N.Y. Apr. 4, 2007).

As with the warrants to search the contents of Mr. Daskal’s phones, *see supra* § III, conspicuously absent from the NY Residence Warrant are meaningful content limitations, such as a subject, name, date, or even time frame, further hallmarks of a particularity deficiency. *See e.g.*, *Zemlyansky*, 945 F. Supp. 2d at 459 (discussing failure to include a time limitation, where such limiting information is available). (*See* Ex. I at 1-2.) Nor can the bare reference to the New York State penal code sections salvage the warrant.⁵ *See e.g.*, *Galpin*, 720 F.3d at 448 (search warrant “facially overbroad” that authorized seizure of “evidence that will constitute, substantiate or support violations of NYS Corrections Law, section 168–f subdivision four, NYS Penal Law and or Federal Statutes”); *George*, 975 F.2d at 75 (warrant authorization to search for “any other evidence relating to the commission of a crime” allowed officers too much discretion). The general statutes provide neither factual detail nor limitation to guide the executing officers, leaving them with nearly unfettered discretion to seize “any and all” of Mr. Daskal’s devices, documents, and personal effects.

C. The NY Residence Warrant Purported to Authorize Search and Seizure of Materials Exceeding any Probable Cause Showing

For similar reasons, the NY Residence Warrant is also overbroad. It improperly granted the executing agents the authority to root around and seize vast categories of Mr. Daskal’s digital and physical documents and effects, although the probable cause showing for Mr. Daskal’s home

⁵ Of course, the government also cannot rely on the affidavit in support of the warrant application, as it was neither attached nor incorporated into the NY Residence Warrant. *See United States v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010) (“we may no longer rely on unincorporated, unattached supporting documents to cure an otherwise defective search warrant.”).

supported, at most, a search for sex toys, letters from the complainant, and communications between Mr. Daskal and the complainant. (See Ex. H ¶¶ 4-9.)

The NY Residence Warrant application did not establish probable cause to seize approximately 30 devices in their entirety, numerous Hebrew blessings and documents from community leaders, rabbis and friends, and other similar personal effect. But that is nonetheless precisely what happened. And it is no surprise: the reason that agents seized extensive swaths of irrelevant materials is because the NY Residence Warrant itself was impermissibly broad on its face. It purported to authorize agents to seize “all computers,” “all handwritten or typed notes,” and all records of “internet usage history” with little limitation. (Ex. I at 1-2.) Such sweep could not be properly circumscribed to materials for which there is probable cause.⁶

Recent cases in this Circuit have deemed similar warrants granting blanket permission to seize virtually anything and everything unconstitutionally overbroad. *United States v. Zemlyansky*, for example, found that a warrant authorizing seizure of “all patient care records, bank account information, and patient appointment information,” from a medical billing office was overbroad. *Zemlyansky*, 945 F. Supp. 2d at 464-65. While the affiant agent in *Zemlyansky* provided probable cause to search and seize materials from the billing office relating to five clinics mentioned in the supporting affidavit, the scope of the warrant’s seizure list was not justified. It authorized search and seizure of “almost everything that one could expect to find at a billing office,” and “unlimited

⁶ The May 10, 2018 NY Residence Warrant, the first warrant issued as to Mr. Daskal, also fails for wholly lacking probable cause. The warrant relies entirely on the word of a complainant with neither a proven track record of truthfulness nor corroboration. See *Wagner*, 989 F.2d at 72-73 (informant should have “a track record of providing reliable information” or be “corroborated in material respects”). The complainant here has neither. The complainant’s alleged firsthand recounting of the incidents cannot make a probable cause showing either: “an informant’s status as an eyewitness does not alone impart an automatic badge of reliability.” *United States v. Zucco*, 694 F.2d 44, 48 (2d Cir. 1982) (quotation marks and citations omitted).

search and seizure of all computers and thumb drives, as well as virtually anything electronic and anything related to the use or operation of those electronics.” *Id.* The warrant was thus “for all practical purposes, a prohibited general warrant to search Tri-State for evidence of a crime.” *Id.* at 459; *accord Wey*, 256 F. Supp. 3d at 393-94 (“the sheer scope of the Warrants—reaching . . . essentially all documents . . . unlimited by relevance to criminal conduct or by timeframe—precludes a finding that the seizure authorization remained within the bounds of the Government’s probable cause showing.”).

The same is true here. As in *Wey* and *Zemylansky*, the allegations in the NY Residence Warrant application do not provide probable cause to support seizure of the comprehensive categories of materials covered by the warrant—particularly as those categories purport to include much or all of Mr. Daskal’s personal digital and handwritten communications, apparently without reference to the crimes under investigation. The NY Residence Warrant fails for overbreadth.

D. The State Authorities’ Unconstitutional Seizure of Approximately 30 Devices Tainted Any Attempt to Search Selected Devices Later Pursuant to a Federal Warrant

Perhaps the most flagrant violation attendant to the search of Mr. Daskal’s residence involves the state authorities’ seizure of approximately 30 computers without probable cause to search or seize any particular computer at all. Nonetheless, the state authorities continued to hold the computers for over a year with neither probable cause nor a valid timely warrant. Only thereafter did the state authorities provide the approximately 30 devices to the federal government and an effort ensued to establish probable cause to search a limited subset of the computers. The belated effort to comply with the Fourth Amendment, however, cures nothing. If anything, the government’s effort to get a second chance only highlights the systematic disregard of the Fourth Amendment that plagued the NY Residence Warrant (like the NY Phones Warrant) from the

outset. The materials seized from Mr. Daskal's residence, including the devices, should be suppressed.

Fundamentally, the NY Residence Warrant lacked probable cause to seize or search *any* of Mr. Daskal's computers—let alone approximately 30. The warrant application made only vague reference to Mr. Daskal's use of computers: that he allegedly “scanned [the complainant's] letters onto his computer,” (Ex. H ¶ 7), without specifically identifying which of the “two laptop computers” and “multiple desktop computers,” (*id.* ¶ 9), may have contained the complainant's correspondence. That is insufficient under the Fourth Amendment to permit search or seizure of *any* computers in Mr. Daskal's home. The Fourth Amendment requires that the warrant establish probable cause for the *particular place*—here, the specific computer—to be searched. *See United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011) (“Th[e] required nexus between the items sought and the ‘particular place’ to be searched protects against the issuance of general warrants[.]”). Because Mr. Daskal's residence contained more than two dozen computers, in the absence of any details identifying *which* of the multiple computers was allegedly used in connection with the charged conduct, the warrant lacked probable cause to search any computer at all. *See, e.g., United States v. Romain*, No. 13-CR-724, 2014 WL 6765831 (RWS), at *4 (S.D.N.Y. Dec. 1, 2014) (“The relevant inquiry then is whether the two Cellphones taken from the Defendant were reasonably likely to contain evidence of the crimes described given the facts in the Application”).

For similar reasons, the warrant also lacked the requisite particularity to seize any of the devices found in Mr. Daskal's home. Because the state authorities apparently had no detail regarding *which* computers were allegedly involved in the communications, and thus which could be properly subject to seizure under the warrant, by definition the NY Residence Warrant could not provide the agents with guidance regarding which devices were subject to seizure as mandated

by the Fourth Amendment. *See Cioffi*, 668 F. Supp. 2d at 390 (“a warrant can violate the [Fourth Amendment] either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries.”). The warrant instead purported to permit search and seizure of virtually all computers and anything they contained, including “any and all computers,” “any and all cellular telephones,” “any and all computer software,” “any and all computer-related documentation,” “any and all data, information, or images evidencing internet usage history,” among other limitless categories. (Ex. I at 1-2.)

Unsurprisingly, blanket seizure of Mr. Daskal’s devices ensued. By their own admission, the state authorities seized “29 or 30 devices.” (Ex. R 3:14.) While the NY Residence Warrant may plausibly provide probable cause to believe that *some* computers could contain the complainant’s communications, there is no reading of the warrant permitting seizure of more than two-dozen devices. *See United States v. Pinto-Thomaz*, 352 F. Supp. 3d 287, 308-09 (S.D.N.Y. 2018) (“Executing agents are considered to have flagrantly disregarded the warrant’s terms where . . . they effect a widespread seizure of items that were not within the scope of the warrant”) (quotation marks and citations omitted).

Compounding the constitutional problems, the authorities took over a year, until the September 2019 Federal Computers Warrant, before even attempting to cure the Fourth Amendment defects—letting the state warrant go stale in the interim, and resulting in warrantless governmental seizure of Mr. Daskal’s devices for an extended period. Although the state authorities seized the approximately 30 devices in May 2018, (*see* Exs. H and I), the state never attempted to either determine which specific devices were potentially subject to probable cause or execute the NY Residence Warrant by commencing searches on the computers. The 15-month period in which the state authorities simply held the 30 devices without ever acquiring or executing

a valid warrant is an independent basis for suppression. *See United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012) (ordering suppression based on “the government’s more than fifteen-month delay in reviewing the seized electronic evidence”).

In August 2019, the state authorities supplied the devices to the federal government. (*See* Ex. T at 2.) Only thereafter, in September 2019—over a year after the state authorities had seized approximately 30 devices—did the government first attempt to identify which of the seized devices allegedly contained the complainant’s correspondence to establish probable cause. (*See* Ex. N ¶ 19.) When the government first met with the complainant in an effort to establish for which of the 30 devices, if any, there was probable cause, nearly two years had passed since the alleged incidents, and the complainant’s memory of specific devices had surely faded. (*See id.*)

At that point, it was too late to cure the indelible constitutional violation of maintaining approximately 30 devices for a year without either probable cause, or a timely warrant. The law does not “allow the government a second chance to fix a problem that never should have arisen.” *Cioffi*, 668 F. Supp. 2d at 398-99 (there is “no way to purge the taint of [the government’s] unconstitutional[] . . . search No court has ever endorsed the view that it would allow the government to retroactively *cure* a Fourth Amendment violation, and it is easy to see why. The violation is not the discovery of incriminating evidence, but the invasion of the searchee’s privacy. Since such a violation is inherently irremediable, the exclusionary rule exists to deter violations in the first instance.”). The devices, and remaining items seized from Mr. Daskal’s home should be suppressed.

V. THE COURT SHOULD ORDER THE GOVERNMENT TO FILE A BILL OF PARTICULARS TO PROVIDE MR. DASKAL WITH ADEQUATE NOTICE OF THE CHARGES AGAINST HIM

On May 23, 2022, defense counsel requested that the government provide particulars regarding the dates of occurrence of each incident encompassed in Count Two (murder for hire

conspiracy), Count Two of the Indictment, which charges him with violating 18 U.S.C. § 2423(a), transporting a minor in interstate commerce with the intent to engage in criminal sexual activity. The government declined, informing the defense as follows: “I can’t say these are the only days we plan to elicit evidence about but I do expect that there will be evidence of trips on or about August 9, August 24, August 28, and August 31, 2017.” (Ex. S.)

Rule 7(f) of the Federal Rules of Criminal Procedure provides that the accused has the right to seek “a bill of particulars in order to identify with sufficient particularity the nature of the charge pending against him, thereby enabling [the] defendant to prepare for trial [and] to prevent surprise.” *United States v. Bortnovsky*, 820 F.2d 572, 574 (2d Cir. 1987). “The purpose of a bill of particulars is to supplement the allegations in the indictment when necessary to (1) enable the defendant to prepare his defense, (2) avoid unfair surprise to the defendant at trial, and (3) preclude a second prosecution of the same offense.” *United States v. Mandell*, 710 F. Supp. 2d 368, 384 (S.D.N.Y. 2010). A bill of particulars is necessary “where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused.” *United States v. Walsh*, 194 F.3d 37, 47 (2d Cir. 1999).

This is a textbook case for requiring a bill of particulars. Without one, Mr. Daskal has no certainty as to which dates involving the alleged victim the government presented to the grand jury, or which incidents the grand jury charged him with. The government’s statement to defense counsel—“I can’t say these are the only days we plan to elicit evidence about”—makes clear that other incidents may be included in the Indictment’s charges.

In other words, based on the Indictment and discovery, Mr. Daskal has no clarity whether the government presented to the grand jury just the four dates mentioned, or whether there were many more? And if there were more dates presented to the grand jury, which? A bill of particulars

is thus required. *See United States v. Gammarano*, No. 06-CR-0072 (CPS), 2007 WL 2077735, at *10 (E.D.N.Y. July 18, 2007) (a bill of particulars required where “the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused.”) (quotation marks and citations omitted).

Understanding the details of the time, place and occurrence of each alleged incident encompassed in Count Two is likewise necessary for any alibi defenses, or other incident-specific defenses that Mr. Daskal may have. Without information as to when the alleged acts took place, Mr. Daskal cannot adequately prepare for trial. *See, e.g., United States v. Siddiqi*, No. 06-CR-377 (SWK), 2007 WL 549420, at *3 (S.D.N.Y. Feb. 21, 2007) (ordering bill of particulars explaining “[i]n the absence of more specific information concerning the approximate dates and amounts of individual bribery payments, Siddiqi will be unreasonably hampered in his ability to prepare a defense. For example, Siddiqi will be unable to offer an alibi if he does not know the dates on which he is alleged to have received bribes.”).

The risk of ambush at trial is amplified further if the government can change its mind at the last moment as to which and how many alleged incidents with respect to the minor female are implicated in the Indictment’s charges.

Accordingly, the Court should order the government to file a bill of particulars to provide Mr. Daskal with adequate notice of the charges against him. Alternatively, the Court should preclude the government from relying upon incidents that occurred on any other dates than the four now identified.

VI. CONCLUSION

Defendant Jacob Daskal respectfully requests that this Court grant his motions and: (1) suppress the fruits of the searches of his cellular telephones; (2) suppress the fruits of the searches of Mr. Daskal's computers; (3) suppress the fruits of the searches of his home; (4) or, in the alternative, hold a suppression hearing regarding the searches of Mr. Daskal's devices and home; and (5) order the government to file a bill of particulars.

Dated: June 2, 2022
New York, New York

Respectfully submitted,

MEISTER SEELIG & FEIN LLP

By: /S/

Henry E. Mazurek
Ilana Haramati
Jason I. Ser

Attorneys for Defendant Jacob Daskal